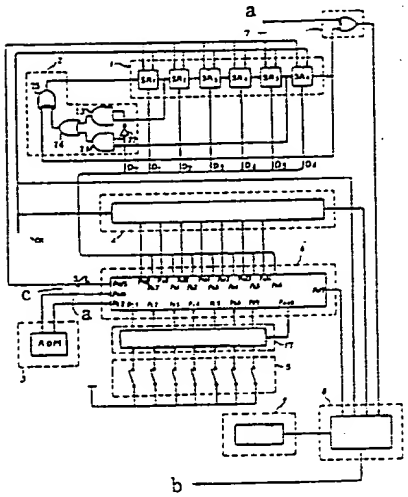
(54) PRIVACY CALL EQUIPMENT
(11) 3-76447 (A) (43) 2.4.1991 (19) JP
(21) Appl. No. 64-212613 (22) 18.8.1989
(71) SHARP CORP (72) JUNJI HIRAIDE(1)
(51) Int. Cl⁵. H04L9/06,H04L9/14

PURPOSE: To sufficiently ensure the secrecy of communication by providing a conversion circuit revising a setting value of a cryptographic key from a cryptographic key setting means so as to revise the cryptographic key differently from each communication thereby revising the setting of the cryptographic key without disturbing the user.

CONSTITUTION: A cryptographic key from a cryptographic key setting means 5 is fed to a microcomputer 6 via a cryptographic key conversion circuit 17 comprising an arithmetic circuit. A data of number of times of communication is fed to the conversion circuit 17 from the microcomputer 6 and the cryptographic key supplied from the cryptographic key setting means 5 is revised to be different from each communication. Thus, it is not required to enter a decoding key at a receiver side and a sender side freely revises the cryptographic key. Then the cryptographic key from the cryptographic key setting means 5 is revised by the conversion circuit 17 different from each communication. Thus, the secrecy of the communication is sufficiently secured without disturbing the user.



CK: clock. a: data. c: address. b: communication line. 20: pseudo random signal generating circuit. 4: parallel serial conversion. 10: serial-parallel conversion. 3: storage circuit. 9: synchronizing signal generation circuit. 8: data control signal switching circuit. 7: cryptographic circuit

E5353

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3-76447

⑤Int.Cl.⁵　識別記号　庁内整理番号　⑬公開　平成3年(1991)4月2日

H 04 L 9/06
9/14

6914-5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 1　(全6頁)

⑭発明の名称　秘話装置

⑳特　願　平1-212613

㉒出　願　平1(1989)8月18日

⑫発明者　平出　順二　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

⑫発明者　多田　順次　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

⑪出願人　シャープ株式会社　大阪府大阪市阿倍野区長池町22番22号

⑭代理人　弁理士　山口　邦夫

明　細　書

1. 発明の名称

秘　話　装　置

2. 特許請求の範囲

(1) 送信側には、

第1の疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記暗号鍵の設定値を変更する変換回路と、

上記疑似ランダム信号発生回路の初期設定データを記憶した第1の記憶回路と、

上記変換回路からの暗号鍵に対応したアドレス信号によって上記第1の記憶回路から上記初期設定データを読み出して上記第1の疑似ランダム信号発生回路を設定する第1の制御手段と、

上記第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられ、

上記暗号化回路の出力データおよび上記アドレス信号が送信され、

受信側には、

上記第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、

上記第1の記憶回路と同じ内容を記憶した第2の記憶回路と、

受信した上記アドレス信号によって上記第2の記憶回路から上記初期設定データを読み出して上記第2の疑似ランダム信号発生回路を設定する第2の制御手段と、

上記第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられることを特徴とする秘話装置。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明は、例えば有線あるいは無線ディジタル通信に使用して好適な秘話装置に関する。

〔従来の技術〕

通信において、通信内容が秘密である場合には秘話通信を行なう必要がある。この場合、送信側

では、通常データ（平文）が暗号化され、この暗号化データ（暗号文）が送信される。そして、受信側では、この暗号文が平文に復号化される。

第５図は、従来の秘話装置を示している。

同図において、送信側では、平文が暗号化回路１３に供給されて暗号鍵に応じて暗号文に変換される。この暗号化回路１３からの暗号文は、有線また無線の通信区間を介して、受信側に供給される。また、受信側では、暗号文が復号化回路１４に供給されてが復号化鍵１６に応じて平文に変換される。

［発明が解決しようとする課題］

第５図例によれば、送信側および受信側が、暗号化および復号化のために、例えば同一の鍵を所有する必要がある。そのため、送信側では暗号鍵を自由に変更することができなかった。しかし、通信の秘密を確保するには、暗号鍵を度々変更する必要がある。

そこで、本出願人は、先に、暗号鍵を自由に変更できる秘話装置を提案した（特願平１－７０２００号）。以下、この秘話装置について説明する。

第２図は送信側のブロック図である。

同図において、２０は疑似ランダム信号発生回路であり、この疑似ランダム信号発生回路２０は、６段のシフトレジスタＳＲ１～ＳＲ６の縦続接続段１と、この縦続接続段１の帰還路を選択する切り替え回路２とで構成される。

縦続接続段１のシフトレジスタＳＲ１～ＳＲ６のロードおよびシフト状態は、制御手段であるマイクロコンピュータ６からの制御信号Ｓ／Ｌによって制御される。制御信号Ｓ／Ｌがロード状態のとき、シフトレジスタＳＲ１～ＳＲ６には、マイクロコンピュータ６からの初期値データＤ１～Ｄ６がロードされる。なお、これらシフトレジスタＳＲ１～ＳＲ６はクロックＣＫに同期して動作するようにされる。

切り替え回路２は、種々のゲートおよびインバータで構成される。すなわち、アンドゲート２１にはシフトレジスタＳＲ５の出力信号が供給されると共に、マイクロコンピュータ６からの制御データＤ７が供給される。また、アンドゲート２３にはシフトレジスタＳＲ１の出力信号が供給されると共に、制御データＤ７がインバータ２２を介して供給される。そして、これらアンドゲート２１および２３の出力信号がオアゲート２４に供給される。したがって、制御データＤ７がハイレベルかローレベルかに応じて、オアゲート２４からはシフトレジスタＳＲ１またはＳＲ５の出力信号が出力される。

また、エクスクルーシブオアゲート２５にはオアゲート２４の出力信号が供給されると共に、シフトレジスタＳＲ６の出力信号が供給される。そして、このエクスクルーシブオアゲート２５の出力信号はシフトレジスタＳＲ１に帰還される。したがって、シフトレジスタＳＲ１～ＳＲ６がシフト動作をするとき、シフトレジスタＳＲ６からは初期値データＤ１～Ｄ６および切り替え回路２の選択に応じた疑似ランダム信号が出力される。

また、５は暗号鍵設定手段であり、この暗号鍵設定手段５は、ハイレベルまたはローレベルを選択する７個の接続スイッチで構成される。この場合、これら７個の接続スイッチの一端は電源端子に接続され、その他端はマイクロコンピュータ６の端子Ｐ11～Ｐ17に接続される。

また、３は例えばＲＯＭ（リードオンリーメモリ）で構成され記憶回路であり、この記憶回路３には縦続接続段１のシフトレジスタＳＲ１～ＳＲ６に供給される初期値データＤ１～Ｄ６と、切り替え回路２に供給される制御データＤ７とが複数組記憶されている。

この場合、暗号鍵設定手段５で設定された暗号鍵に応じたアドレス信号がマイクロコンピュータ６より記憶回路３に供給され、対応する初期値データＤ１～Ｄ６および制御データＤ７が読み出される。そして、この初期値データＤ１～Ｄ６および制御データＤ７はマイクロコンピュータ６の端子Ｐ01～Ｐ07を介してシフトレジスタＳＲ１～ＳＲ６および切り替え回路２に供給され、これにより疑似ランダム信号発生回路２０が初期設定される。

また、マイクロコンピュータ６からのアドレス信号はパラレル／シリアル変換回路４でシリアル信号に変換されて出力される。

また、７はエクスクルーシブオアゲートで構成される暗号化回路であり、この暗号化回路７には、疑似ランダム信号発生回路２０からの疑似ランダム信号と、データ発生手段（図示せず）からのシリアルデータ（例えば、音声データ）とが供給されて、シリアルデータは暗号化される。

また、８はデータ／制御信号切り替え回路であり、この切り替え回路８には変換回路４より出力されるアドレス信号、暗号化回路７より出力される暗号化データおよび同期信号発生回路９からの同期信号が供給される。そして、マイクロコンピュータ６の制御により、これらの信号はクロックＣＫに同期して切り替えられ、有線または無線の通信回線に出力される。第４図はその通信信号の構成例を示している。

このように、送信側では、暗号鍵設定手段５による暗号鍵の設定に応じて、データが暗号化され、同期信号およびアドレス信号と共に、通信回線に出力される。

第３図は、受信側のブロック図である。この第３図において、第２図と対応する部分には同一符号を付して示している。

同図において、通信回線からの信号はデータ／制御信号切り替え回路８を介して同期信号検出回路１２に供給され、この同期信号検出回路１２で検出される同期信号（第４図参照）はマイクロコンピュータ６に供給される。

また、切り替え回路８には、マイクロコンピュータ６より同期信号に応じて制御信号およびクロックが供給される。そして、通信回線からの信号に含まれるアドレス信号は切り替え回路８よりシリアル／パラレル変換回路１０でパラレル信号に変換されたのちマイクロコンピュータ６に供給される。そして、このアドレス信号はマイクロコンピュータ６より記憶回路３に供給され、対応する初期値データＤ１～Ｄ６および制御データＤ７が読み出される。そして、この初期値データＤ１～Ｄ６および制御データＤ７はマイクロコンピュータ６の端子Ｐ01～Ｐ07を介してシフトレジスタＳＲ１～ＳＲ６および切り替え回路２に供給される。これにより疑似ランダム信号発生回路２０が初期設定される。

この場合、受信側および送信側の記憶回路３の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路２０は同じ構成であるので、受信側の疑似ランダム信号発生回路２０からは、送信側と同様の疑似ランダム信号が発生される。

また、１１はエクスクルーシブオアゲートで構成される復号化回路である。この復号化回路１１には、疑似ランダム信号発生回路２０からの疑似ランダム信号と、切り替え回路８からの暗号化データとが供給され、暗号化データは復号化されて出力される。

このように第２図および第３図に示す秘話装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

しかし、暗号鍵の設定はユーザーによって行なわれるものであり、ユーザーがその設定値を変更しない限り、疑似ランダム信号発生回路２０からは常に同じ疑似ランダム信号が発生されて暗号化される。したがって、一度、第３者によって解読されると、通信の秘密を確保できなくなる。

そこで、この発明では、ユーザーを煩わせることなく、通信の秘密を充分に確保できる秘話装置を提供するものである。

［課題を解決するための手段］

この発明による秘話装置は以下のように構成される。すなわち、

送信側には、第１の疑似ランダム信号発生回路と、暗号鍵を設定する暗号鍵設定手段と、暗号鍵の設定値を変更する変換回路と、疑似ランダム信号発生回路の初期設定データを記憶した第１の記憶回路と、変換回路からの暗号鍵に対応したアドレス信号によって第１の記憶回路から初期設定データを読み出して第１の疑似ランダム信号発生回路を設定する第１の制御手段と、第１の疑似ラン

ダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられる。そして、暗号化回路の出力データおよびアドレス信号が送信される。

また、受信側には、第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、第1の記憶回路と同じ内容を記憶した第2の記憶回路と、受信したアドレス信号によって第2の記憶回路から初期設定データを読み出して第2の疑似ランダム信号発生回路を設定する第2の制御手段と、第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられる。

〔作　用〕

上述構成においては、暗号鍵設定手段5からの暗号鍵の設定値を変更する変換回路17が設けられる。この変換回路17で暗号鍵は、例えば通信ごとに異なるように変更される。したがって、ユーザーを煩わせることなく暗号鍵の設定変更が行なわれ、通信の秘密を充分に確保できるようになる。

〔実　施　例〕

以下、第1図を参照しながら、この発明の一実施例について説明する。この第1図において、第2図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例においては、暗号鍵設定手段5からの暗号鍵は演算回路で構成される暗号鍵変換回路17を介してマイクロコンピュータ6に供給される。変換回路17にはマイクロコンピュータ6より通信回数のデータが供給され、暗号鍵設定手段5より供給される暗号鍵は通信ごとに異なるように変更される。

このように変更するための演算処理例としては、通信ごとに「1」を加算していくというような簡単なものから、PN発生回路によるスクランブル化、乗算、除算や各種演算による複雑なものまで考えられる。

本例は以上のように構成され、その他の部分は第2図例と同様に構成される。なお、受信側は第3図例と同様に構成される。

本例によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。そして、暗号鍵設定手段5からの暗号鍵は変換回路17で通信ごとに異なるように変更される。したがって、ユーザーを煩わせることなく、通信の秘密を充分に確保することができる。

なお、上述実施例においては、縦続接続段1のシフトレジスタの段数は6段とされたものであるが任意の段数とすることができる。また、シフトレジスタSR1に帰還する信号は、上述実施例に限定されることなく任意のシフトレジスタの出力とすることができる。

〔発明の効果〕

以上説明したように、この発明によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができると共に、暗号鍵設定手段からの暗号鍵は変換回路で、例えば通信ごとに異なるように変更されるので、ユーザーを煩わせることなく、通信の秘密を充分に確保することができる。

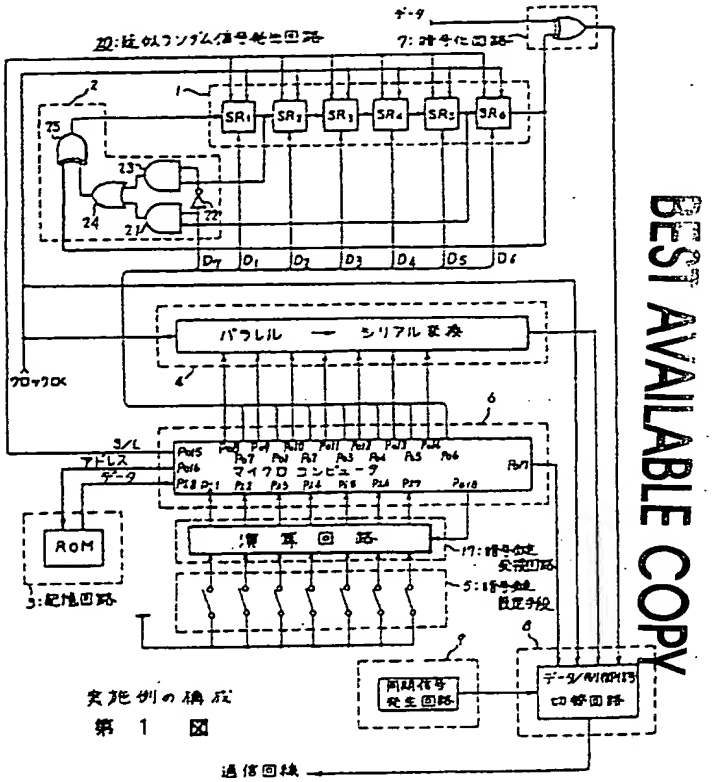
4．図面の簡単な説明

第1図はこの発明の一実施例を示すブロック図、第2図は秘話装置の送信側のブロック図、第3図は秘話装置の受信側のブロック図、第4図は通信信号の構成を示す図、第5図は従来の秘話装置のブロック図である。

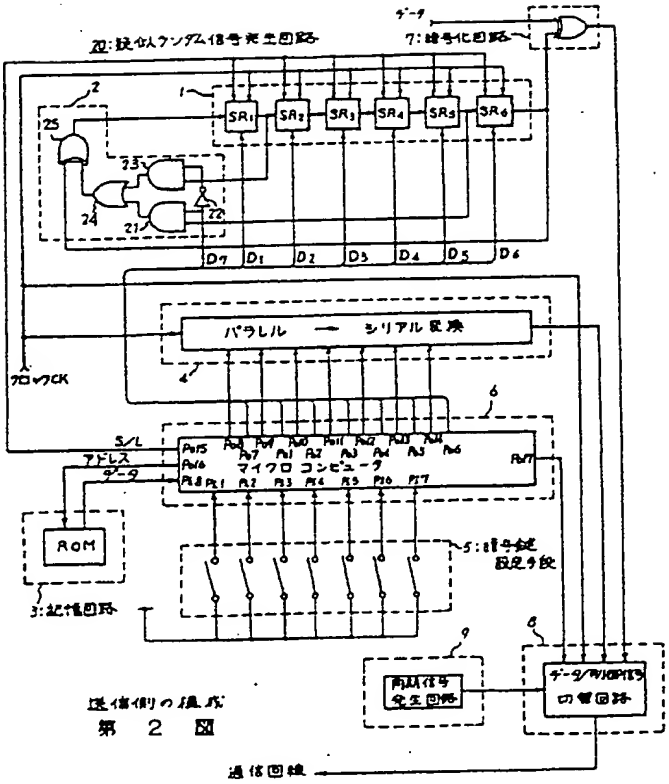
3・・・記憶回路
4・・・パラレル／シリアル変換回路
5・・・暗号鍵設定手段
6・・・マイクロコンピュータ
7・・・暗号化回路
8・・・データ／制御信号切り替え回路
9・・・同期信号発生回路
10・・・シリアル／パラレル変換回路
11・・・復号化回路
12・・・同期信号検出回路
17・・・暗号鍵変換回路

20・・・疑似ランダム信号発生回路

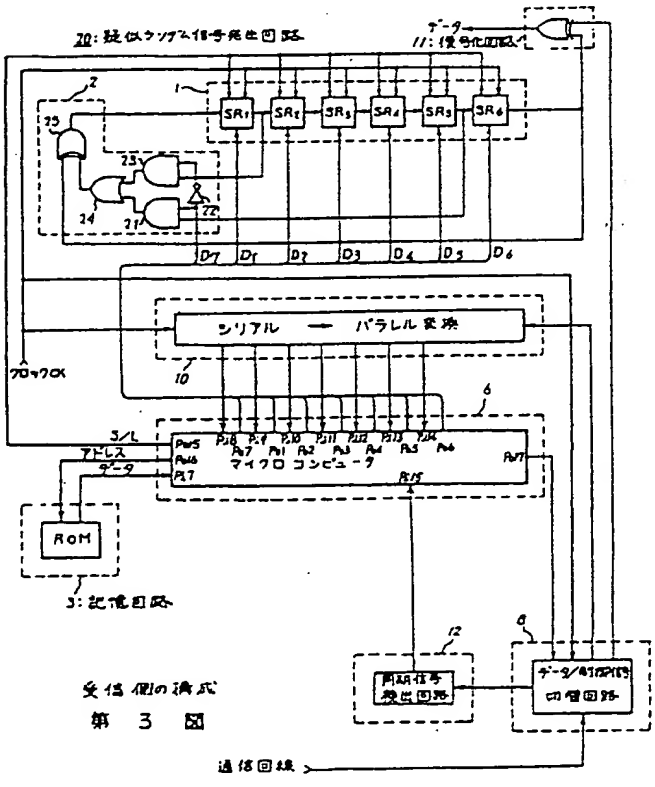
特許出願人　シャープ株式会社
代理人　弁理士　山口邦夫



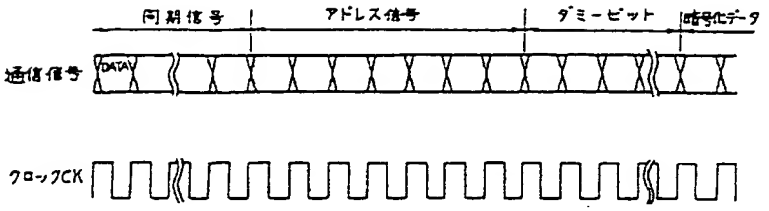
実施例の構成
第 1 図



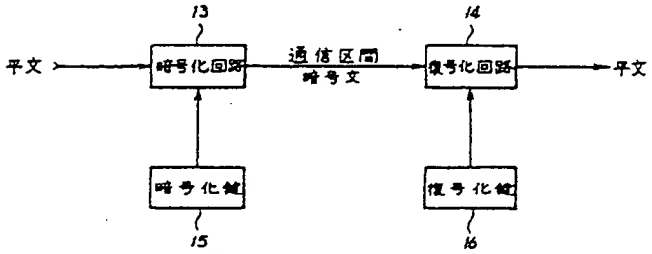
送信側の構成
第 2 図



受信側の構成
第 3 図



通信信号の一例
第 4 図



従来例の構成図
第 5 図